US010003975B2

(12) **United States Patent**
Kremer et al.

(10) **Patent No.: US 10,003,975 B2**
(45) **Date of Patent: *Jun. 19, 2018**

(54) **AUTHORIZED AREAS OF AUTHENTICATION**

(71) Applicant: **Finjan Mobile, Inc.**, East Palo Alto, CA (US)

(72) Inventors: **Alexander Lin Kremer**, San Mateo, CA (US); **Geoffrey House**, San Francisco, CA (US); **Lee McDole**, Oakland, CA (US); **Michael Godlewski**, San Francisco, CA (US); **Rudolph Mutter**, Millbrae, CA (US); **Timothy Shipman**, San Francisco, CA (US); **Jules Panopoulos**, Mountain View, CA (US)

(73) Assignee: **Finjan Mobile, Inc.**, East Palo Alto, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days. days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/686,111**

(22) Filed: **Aug. 24, 2017**

(65) **Prior Publication Data**

US 2017/0353861 A1   Dec. 7, 2017

Related U.S. Application Data

(63) Continuation of application No. 15/371,396, filed on Dec. 7, 2016, now Pat. No. 9,749,867, and a (Continued)

(51) **Int. Cl.**
H04L 29/06   (2006.01)
H04W 12/08   (2009.01)
(Continued)

(52) **U.S. Cl.**
CPC .... *H04W 12/08* (2013.01); *H04L 63/083* (2013.01); *H04L 63/0861* (2013.01); (Continued)

(58) **Field of Classification Search**
CPC H04W 12/08; H04W 4/02; H04W 12/06; H04W 4/021; H04L 63/108; H04L 63/083; H04L 63/0861; H04L 63/107
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,090,351 B2   1/2012   Klein
8,295,898 B2   10/2012   Ashfield et al.
(Continued)

OTHER PUBLICATIONS

PCT/US16/38592, International Search Report and Written Opinion, dated Aug. 5, 2016, 10 pages.
(Continued)

Primary Examiner — Michael Pyzocha
(74) *Attorney, Agent, or Firm* — Soquel Group I.P Ltd

(57)   **ABSTRACT**

An electronic device including a memory storing at least one of biometric or passcode data of a user, and a processor (i) requesting access of data over the secure network, wherein access to the data is controlled by a server, (ii) scanning biometric or passcode data of the user and validating the scanned biometric or passcode data with the biometric or passcode data of the user stored in said memory, (iii) validating the biometric or passcode data of the user, and (iv) contingent upon the validation being affirmative, submitting a request to the server to generate an authorized area of authentication (AAA) that includes the current location of the electronic device, wherein the server enables access to the secure data only when the location of the electronic device remains within the AAA.

12 Claims, 13 Drawing Sheets